Министерство образования Республики Беларусь
Учреждение образования
Белорусский государственный университет
информатики и радиоэлектроники

УДК 004.056:519.254

Ярук
АндрейМихайлович

Исследование физических генераторов случайных чисел методами статистического тестирования

АВТОРЕФЕРАТ

на соискание степени магистра технических наук
по специальности 1-98 80 01 Методы и системы защиты,
информационная безопасность

Научный руководитель
Корзун А.И.
Кандидат т.н., доцент

Минск 2015

Библиотека БГУИР

ВВЕДЕНИЕ

В настоящее время последовательности случайных чисел (ПСЧ) находят весьма широкое применение при решении прикладных задач в области математической статистики, численных методов оптимизации, имитационном моделировании, создании и тестировании различных датчиков и систем и т. д.

Стремительное развитие информационных технологий привело к формированию глобальной информационной среды. Важнейшей проблемой информатизации является обеспечение точности и безопасности информации. Особую роль при разработке систем обеспечения информационной безопасности играют ПСЧ. Используемые в них криптографические механизмы предъявляют предельно «жесткие» требования к качеству ПСЧ.

К основным задачам, требующим эффективного решения, относятся проблемы электронной бесконтактной идентификации объектов, аутентификации, управления доступом, защиты каналов передачи информации и трафика.

Таким образом, на современном этапе развития технологии защиты информации основной задачей является повышения надежности методов оценки качества генераторов случайных чисел (ГСЧ).

В настоящее время в Республике Беларусь реализуется программа «Электронное правительство», в соответствии с которой каждому гражданину необходимо свой идентификатор для осуществления процедуры электронной цифровой подписи (ЭЦП). Реализация ЭЦП происходит с использованием ключей шифрования, которые определяют надежность криптографических процедур. Надежные ключи вырабатывают физические ГСЧ. Физические ГСЧ содержат электронные пластиковые карты (ЭПК), в которых организована уникальная защита ключей. В связи с этим статистическое тестирование ГСЧ ЭПК как потенциальных источников криптографических ключей актуально.

Целью данной работы является тестирование ГСЧ ЭПК с использованием одной из существующих тестовых подборок. Для достижения данной цели были поставлены задачи:

– выбор средств тестирования;

– получение ПСЧ чисел из различных ЭПК;

– тестирование ПСЧ;

– реализация алгоритмов тестирования в среде программирования Matlab и JavaScript.

Библиотека БГУИР

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Целью данной работы является тестирование ГСЧ ЭПК с использованием одной из существующих тестовых подборок. Для достижения данной цели были поставлены задачи:

– выбор средств тестирования;

– получение ПСЧ чисел из различных ЭПК;

– тестирование ПСЧ;

– реализация алгоритмов тестирования в среде программирования Matlab и JavaScript.

. Объектом исследования в магистерской диссертации выступают – ГСЧ и их оценка на основании выбранного тестовогостандарта FIPS 140-2.Проведено экспериментальное исследование ГСЧ пяти ЭПК по тестам стандарта FIPS 140-2 с использованием двух выбранных программных сред Matlab и JavaScript.

Положения, выносимые на защиту

1. Реализация методов тестирования по стандарту FIPS 140-2 на языках программирования Matlabи JavaScript.

2. Сформирован аппаратно-программный комплекс для формирования последовательности случайных чисел из ЭПК и для тестирования полученных последовательностей с использованием стандарта FIPS 140-2.

Личный вклад соискателя

1. Сформированы алгоритмы тестирования, с помощью которых реализованы тесты стандарта FIPS 140-2 в средах Matlabи JavaScript.

2. Результаты тестирования позволили сделать вывод о том, что реализация алгоритмов на основе JavaScriptпозволяет ускорить процесс тестирования в 60 раз.

Библиотека БГУИР

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

Общий объем магистерской диссертации составляет 85страниц, включая 15 иллюстраций, 9 таблицы, библиографический список из 23 наименований, 2 приложения. Работа состоит из реферата, введения, трех глав, заключения и приложений.

Во введении отмечены актуальность темы исследования, цель и задачи дипломной работы.

В первой главе рассматриваются основы построения ГСЧ, приведены основные классы генераторов, а также на основе физических генераторов рассмотрен принцип работы. Показаны отличительные особенности устройства ГСЧ ЭПК.

Вторая глава посвящается выбору средств тестирования ГСЧ ЭПК. Рассмотрены наиболее используемые тестовые подборки и для оценки качества работы ГСЧ ЭПК использованы тесты, определенные стандартом FIPS 140-2. Для получения возможности извлечения случайных чисел из ГСЧ ЭПК и их тестирования был сформирован специальный аппаратно-программный комплекс, включающий в себя среду программирования MATLAB и JavaScript.

В третьей главе проведено экспериментальное исследование пяти массивов случайных чисел, извлеченных из ГСЧ ЭПК. Экспериментальное исследование включало в себя разработку алгоритмов тестирования по FIPS 140-2 в двух программных средах Matlab и JavaScript и анализ их результатов. Для проведения исследования разработаны алгоритмы тестирования по заданным тестам в среде программирования MATLAB и JavaScript.

Практическая значимость работы заключается в формировании АПК, позволяющего извлекать случайные последовательности из ГСЧ ЭПК и исследовать их по тестам стандарта FIPS 140-2.

В заключении даны общие выводы по работе и предложения.

Библиотека БГУИР

ЗАКЛЮЧЕНИЕ

В соответствии с поставленными задачами в данной магистерской диссертации рассмотрены следующие вопросы.

Генерирование случайных последовательностей с заданным вероятностным законом и проверка их адекватности — одни из важнейших проблем современной криптологии. Генераторы случайных последовательностей используются в существующих криптосистемах для генерации ключевой информации и задания ряда параметров криптосистем.

Физические ГСЧ содержат электронные пластиковые карты, в которых организована уникальная защита ключей. В связи с этим статистическое тестирование ГСЧ ЭПК как потенциальных источников криптографических ключей актуально.

Таким образом, в ходе магистерской диссертации проведено экспериментальное исследование пяти массивов случайных чисел, извлеченных из ГСЧ ЭПК. Экспериментальное исследование включало в себя разработку алгоритмов тестирования по FIPS 140-2 в двух программных средах Matlab и JavaScriptи анализ их результатов.

Основываясь на полученных результатах можно сделать вывод о том, что ГСЧ ЭПК пригодны для использования в криптографических системах защиты информации.

Исходя из результатов сравнения двух программных средств, суммарное время, затраченное на тестирование в программе, написанной на JavaScript примерно в 60 раз меньше, чем в Matlab. Еще одним преимуществом использования языка JavaScript является возможность хранения алгоритмов тестирования на удаленных веб-серверах, и в случае необходимости могут быть вызваны оператором ПК.

Библиотека БГУИР

СПИСОК ОПУБЛИКОВАННЫХ РАБОТ

По теме магистерской диссертации были опубликованы следующие работы:

1. Ярук А.М. Системы статистического тестирования генераторов случайных чисел/ Ярук А.М., Киевец Н.Г.// Материалы XIX Международной научно-практической конференции «Современные средства связи»: тезисы доклада – Минск: ВГКС, 14-15 октября 2014, – С 197.

2. Ярук А.М. Разработка программных средств статистического тестирования/ Ярук А.М., Киевец Н.Г., Корзун А.И. //Материалы 51-й научной конференции аспирантов, магистрантов и студентов «Телекоммуникационные системы и сети»: тезисы доклада – Минск: БГУИР, 13-17 апреля 2015, – С 23.

3. Ярук А.М. Проверка качества работы генератора случайных чисел. / Ярук А.М., Киевец Н.Г., Корзун А.И. // Технические средства защиты информации: Тезисы докладов XIII Белорусско-российской научно-технической конференции, 4–5 мая 2015 г., Минск. Минск: БГУИР, 2015. — С.50-51.

Библиотека БГУИР